

AFFIDAVIT

I, Richard F. Atwood, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. I make this affidavit in support of an application for search warrants to search the following individual and locations:¹

- a. 2 Janes Street, Providence, RI 02905 (hereinafter referred to as the “**TARGET LOCATION**”), as more fully described in Attachment A-1, for the items described in Attachment B.
- b. A GRAY 2017 HONDA ACCORD, SPECIAL EDITION, VIN: 1HGCR2F16HA076280, Delaware temporary registration: [REDACTED] 4216. (hereinafter referred to as the “**SUBJECT VEHICLE**”), as more fully described in Attachment A-2, for the items described in Attachment B.

2. The investigation associated with this application involves Juan Bautista ROSARIO SANDOVAL, Duralline AZCONA RODRIGUEZ, Nahun Martinez Guerrero (herein referred to as “**MARTINEZ GUERRERO**”) and others yet identified. These individuals are suspected of violating federal laws including Title 18, United States Code, § 111(a) (Assaulting, resisting, or impeding certain officers or employees), Title 18, United States Code, § 2114(a) (assault with intent to rob mail matter) and Title 21, United States Code, Sections 841(a) (1) and 846 (drug trafficking and conspiracy) (herein referred to as the **SPECIFIED FEDERAL OFFENSES**). For the reasons set forth in this affidavit, I submit that probable cause exists to believe that the above-mentioned locations contain evidence of the above-listed offenses.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested search warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

¹ A description of the residence and the vehicle to be searched are attached hereto as Attachment A-1 thru A-2 respectively. A list of items to be seized is attached hereto as Attachments B.

II. BACKGROUND OF AFFIANT

4. I am a United States Postal Inspector employed by the United States Postal Inspection Service (USPIS), Boston Division, Rhode Island Domicile and have been so employed since June 2016. I have authority to enforce the criminal laws of the United States and to make arrests. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

5. I have been a law enforcement officer for over twenty-two (22) years. I was also previously a U.S. Postal Inspector from June 2003 to August 2009. In my capacity as a U.S. Postal Inspector, I investigate a wide variety of offenses and violations of federal criminal law, including offenses involving the transportation of controlled substances and other contraband through the United States Postal Service. From August 2009 to June 2016, I was a Special Agent with the Department of Homeland Security (DHS), U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Office of the Special Agent-in-Charge, Boston (SAC/BOS), Airport/Seaport Group. In that position, I investigated a variety of offenses including violations involving contraband being imported and exported into and out of the United States. I received training by the USPIS in the investigation of contraband, including stolen goods, narcotics, and counterfeit documents being transported through the United States mails, and in addition, I received training by HSI in the investigation of smuggled goods and/or contraband over interstate and international lines. Prior to becoming a U.S. Postal Inspector, I was a Police Officer with the Phoenix Police Department for approximately four years, and a Manchester, New Hampshire Police Officer for approximately eight months. Finally, I have a Bachelor of Arts Degree in History that I received while attending Framingham State College, in Framingham, Massachusetts.

6. In my capacity as a Postal Inspector/Special Agent for eighteen (18) years, I have conducted or participated in hundreds of investigations involving the illegal manufacture, smuggling, and distribution of contraband, to include controlled substances, counterfeit merchandise and stolen goods. I have appeared before US District Court Judges in the Districts of Massachusetts, Rhode Island, California and Arizona on numerous occasions to swear to affidavits in support of search, arrest, and seizure warrants pertaining to the illegal manufacture, smuggling, and distribution

of contraband, to include controlled substances, counterfeit merchandise and stolen goods and identities.

7. I have written and/or participated in the execution of numerous search warrants resulting in the seizure of large quantities of controlled substances and paraphernalia involved in the manufacture and distribution of controlled substances; United States currency; records of narcotics and monetary transactions; and drug customer lists and other documents relating to the manufacturing, transportation, ordering, purchasing and distribution of controlled substances, as well as the collection, expenditure, accounting, transportation, and laundering of drug proceeds. I have participated in the debriefing of numerous defendants, informants, and witnesses who had personal knowledge regarding large-scale narcotics trafficking organizations. I have participated in all aspects of drug investigations including conducting surveillance, executing searches pursuant to court-ordered search warrants, and executing arrests. I have received extensive specialized training in the field of controlled substance identification, investigation, and enforcement.

III. PROBABLE CAUSE

A. Summary of the Investigation

8. On September 18, 2021, a United States Postal Service (herein USPS) letter carrier (herein referred to as VICTIM 1) was delivering mail on a postal route in Providence, Rhode Island, when she was approached by three individuals looking for a Priority Mail Express Parcel (PMEP) addressed to [REDACTED]. VICTIM 1 stated when she first arrived, she was carrying the PMEP and was looking for the address. VICTIM 1 stated she was approached by a Hispanic male, heavy set, with a hair bun (herein referred to as SUSPECT 3) asking about the PMEP. Upon locating the address, VICTIM 1 attempted to deliver the PMEP but the name on the parcel was not associated with the address.

9. At that point VICTIM 1 stated she returned to her fully marked USPS vehicle and noticed, what she described as a "PT Cruiser" looking vehicle, with something red on the windshield parked behind her. VICTIM 1 stated she was sitting in her vehicle when one of the unknown Hispanic males (herein referred to as SUSPECT 1) approached her by her driver's side window. VICTIM 1 stated SUSPECT 1 showed her a photo from his cell phone, which contained a USPS receipt that had the tracking number for the PMEP listed on it. SUSPECT 1 also showed VICTIM 1

a picture of the PMEP label, which listed the intended recipient. VICTIM 1 stated she told SUSPECT 1 she needed to see an ID in order to give him the parcel. SUSPECT 1 proceeded to show VICTIM 1 an ID that she described as a school ID but the name listed on the ID, which she remembered being Juan Bautista did not match the name on the PMEP; so, VICTIM refused to give SUSPECT 1 the PMEP. At that point, VICTIM 1 stated SUSPECT 1 started to grab her and pull at her car door to open it.

10. VICTIM 1 stated while SUSPECT 1 was grabbing at her, a second unknown Hispanic male (herein referred to SUSPECT 2) opened the passenger side door and proceeded to punch her in the face. VICTIM 1 stated she was able to strike SUSPECT 2 with her USPS issued scanner but SUSPECT 2 was able to grab the PMEP and then ran off. VICTIM 1 stated she followed SUSPECT 2 in her USPS vehicle while SUSPECT 2 ran down Homer Street, which was directly across the street from [REDACTED]. VICTIM 1 stated she pleaded with SUSPECT 2 to “just give the parcel back” but VICTIM 1 stated SUSPECT 2 pulled out a knife with an orange handle. VICTIM 1 stated SUSPECT 2 did not approach her with the knife but made stabbing motions in her direction.

11. VICTIM 1 stated she continued to follow SUSPECT 2 while he was carrying the PEMP and saw that he was talking on a cell phone, when suddenly a gray Honda Accord with a temporary Delaware license plate pulled up. VICTIM 1 stated SUSPECT 2 got into the back seat of the Honda Accord, with the PMEP and left the area.

12. VICTIM 1 stated she contacted the police after SUSPECT 2 left the area. Providence Police responded to the area but were not able to locate the vehicle the suspects fled in. While speaking to Providence Police, VICTIM 1 was checking her vehicle when she located a black cell phone on the driver’s side floorboard. VICTIM 1 stated the cell phone did not belong to her. Given VICTIM 1’s description of SUSPECT 1’s actions, I believe in my training and experience that the cell phone found on the driver’s side floorboard was the cell phone SUSPECT 1 used to show her a telephone with a picture of the USPS tracking information related to the PMEP. Upon finding the cell phone, which was locked, Inspectors could view Spanish text on the front screen.

13. A subsequent search of USPS databases revealed the PMEP VICTIM 1 was attempting to deliver to [REDACTED] was shipped from Trujillo Alto, Puerto Rico on September 17, 2021. The weight of the PMEP was approximately 6 pounds, 9 ounces and was shipped express, for overnight delivery. Based on my training and experience, Puerto Rico is a known drug source territory. Additionally, I am aware drug dealers often utilize the USPS express, overnight delivery service to ship controlled substances. I am further aware that drug dealers utilize the USPS tracking system to track their parcels not only to ensure they arrive in a timely manner but also to determine exactly when the parcel is delivered. In my training and experience, I also know that US Postal employees have been attacked while delivering parcels suspected of containing controlled substances.

14. Inspectors were able to obtain video surveillance recordings from several businesses in the immediate area, which captured the incident. Surveillance video from a pawn shop directly across the street from 1402 Broad Street captured the “PT Cruiser” looking vehicle, that VICTIM 1 described pulling in behind VICTIM 1’s vehicle approximately one minute after it arrived. It should be noted the “PT Cruiser” looking vehicle was in fact a Honda CRV, bearing Rhode Island registration [REDACTED] 464 (herein referred to as the “Honda CRV RI reg. [REDACTED] 464”). As the driver, SUSPECT 3 exited the Honda CRV RI reg. [REDACTED] 464, the Honda Accord pulled up next to SUSPECT 3 and appeared to have a quick conversation with SUSPECT 3.

15. Additional surveillance video obtained from a salon and day care that were located next to 1402 Broad Street captures SUSPECT 3 speaking to VICTIM 1. SUSPECT 3 was wearing a red shirt, gray sweatpants, flip flops and based on VICTIM 1’s description did in fact have a hair bun. SUSPECT 3 then proceeds to walk down the sidewalk, on his cell phone and approaches the Honda Accord, which was now parked. The video surveillance shows SUSPECT 2 with his right arm out of the passenger side window motioning for SUSPECT 3 to walk over to the car. Then, SUSPECT 2 exits the passenger seat of the Honda Accord and also walks down the sidewalk towards SUSPECT 3. The video surveillance captures SUSPECT 2 and SUSPECT 3 slapping hands and talking to each other. SUSPECT 2 continues to walk towards VICTIM 1, while SUSPECT 3

points towards VICTIM 1's direction. At that point the driver of the Honda Accord, SUSPECT 1, exits the vehicle and speaks to SUSPECT 3 as well.

16. The video surveillance captures the TARGET SUSPECTS walking towards VICTIM 1, when SUSPECT 1 and SUSPECT 2 proceed to assault and rob VICTIM 1 of the PMEP. SUSPECT 1 runs back towards the Honda Accord while SUSPECT 3 gets back into Honda CRV RI reg. [REDACTED] 464 and leave the area. It should be noted, the Honda Accord, driven by SUSPECT 1 nearly struck the Honda CRV RI reg. [REDACTED] 464 as they were fleeing the area. The Honda CRV RI reg. [REDACTED] 464 made an immediate right turn onto Morton Street, while the Honda Accord continued down Broad Street. SUSPECT 2 ran down Homer Street with the PMEP and eventually gets back into the Honda Accord, which was still driven by SUSPECT 1.

17. After several hours of canvassing the area, Inspectors observed the Honda CRV RI reg. 1BS464 return to the area and park in the same spot it was observed earlier. The driver, SUSPECT 3 exited the vehicle; however, this time he was wearing a black shirt and jeans shorts but was still wearing flip flops. SUSPECT 3, after a few minutes, left the area in the Honda CRV RI reg. [REDACTED] 464. Inspectors were able to obtain the license plate for the Honda CRV RI reg. [REDACTED] 464², which listed the registered owner as Euris Abel Peralta Vizcaino (herein referred to as VIZCAINO), who resided on Whitmarsh Street in Providence. Inspectors obtained VIZCAINO's Rhode Island driver's license photograph and determined it was not SUSPECT 3.

18. After obtaining the parcel information that was stolen from VICTIM 1, I used USPS proprietary databases and learned that either the same individual or device querying the status of the stolen PMEP was also querying the status of a PMEP addressed to [REDACTED] Union City, New Jersey, leading me to conclude that the parcels are related³. I have found in my training and experience that even when parcels containing narcotics are shipped to different areas to avoid law enforcement detection, one individual will monitor the parcels to ensure that they arrive on a timely basis and are not interdicted by law enforcement. Additionally, the same USPS proprietary

² Please refer to paragraph 14 for the license plate of SUBJECT VEHICLE 1.

³ It should be noted, Postal Inspectors in Newark, NJ located the Union City parcel and applied for and obtained a federal search warrant for the parcel. Upon executing the warrant, Inspectors discovered 2.205 kilograms of cocaine within the parcel.

databases revealed that either the same individual or device had previously queried a Priority Mail Express Parcel, tracking number EJ584888119US (herein referred to as the JANES ST PARCEL) that was delivered to 4 Janes Street Providence, Rhode Island on August 25, 2021. The JANES STREET PARCEL was shipped from Dorado, Puerto Rico, weighing approximately 18 pounds 10 ounces.

19. On the same day, after recovering the cell phone from VICTIM 1's USPS vehicle, I applied for and obtained a search warrant for the cell phone. The Honorable Patricia A. Sullivan authorized the search of the dropped cell phone⁴. On September 20, 2021, I provided the cell phone to Providence Police Detective Ted Michael for analysis. Detective Michael advised the phone was not supported for a "brute force" extraction so he was unable to complete a full extraction. Det. Michael did however provide the phone number associated with the cell phone, which was [REDACTED]-7041.

20. On September 21, 2021, based on the information I obtained, I requested and served a subpoena on T-Mobile to provide the records of the individual or device tracking the stolen PMEP. I also requested and served T-Mobile a subpoena requesting the subscriber records and tolls on the dropped cell phone.

21. On September 22, 2021, T-Mobile responded and provided the information on both requests, which are as followed:

Cell phone tracking the PMEP: [REDACTED]-9032

Subscriber for the dropped cell phone: TracFone, activated on July 30, 2021

22. On September 22, 2021, I requested and served a subpoena to T-Mobile requesting subscriber records and tolls on the following phone number: [REDACTED]9032. On September 24, 2021, T-Mobile responded and provided the following information:

Subscriber for [REDACTED]-9032: TracFone, activated on August 15, 2021.

23. On September 23, 2021, at approximately 9:15 am, while canvassing the area around Broad Street and Whitmarsh Street for the vehicles involved in the robbery, Inspectors located the

⁴ Please refer to case no.: 21-SW-481-PAS.

Honda CRV RI reg. [REDACTED] 464 parked in front of 22 Adelaide Avenue, Providence. Inspectors immediately established surveillance on the Honda CRV RI reg. [REDACTED] 464. At approximately 11 am, I observed an unknown Hispanic male, exit a bodega at the corner of Broad Street and Adelaide Avenue, wearing a black baseball hat, black shirt, jogger pants and rubber gloves. The unknown Hispanic male was carrying a set of keys and got into the Honda CRV RI reg. [REDACTED] 464. The unknown Hispanic male made a U-turn in the middle of Adelaide Avenue and parked the Honda CRV RI reg. [REDACTED] 464 right next to the bodega. It should be noted, the unknown Hispanic male did not resemble the registered owner, VIZCAINO, or SUSPECT 3. On the same date, the Honorable Patricia A. Sullivan authorized the installation of GPS Tracker on the Honda CRV RI reg. [REDACTED] 464⁵. Inspectors installed the GPS Tracker later that day.

24. Inspectors began to view open source information on the registered owner, VIZCAINO of the Honda CRV RI reg. [REDACTED] 464 and discovered several Facebook photos containing images of VIZCAINO standing with SUSPECT 3, who was linked to the photo by the name “Jimmy Azcona.” Inspectors attempted to locate identifying information for “Jimmy Azcona” but were unsuccessful.

25. On October 13, 2021, while conducting surveillance on the Honda CRV RI reg. [REDACTED] 464, RI State Police Detectives and USPIS Task Force Officers (TFOs) Juan Coronado and Justin Andreozzi witnessed “Jimmy Azcona” driving the Honda CRV RI reg. [REDACTED] 464 after it left the area of Whitmarsh Street. Detectives Coronado and Andreozzi followed the Honda CRV RI reg. [REDACTED] 464 for a short time but the Honda CRV RI reg. [REDACTED] 464 eventually returned to the Whitmarsh Street area and parked in the back of the residence at [REDACTED].

26. On October 14, 2021, Inspectors conducted surveillance on the Honda CRV RI reg. [REDACTED] 464 as it left [REDACTED]. Inspectors followed the Honda CRV RI reg. [REDACTED] 464 to area of Waldo Street and Sorrento Street, where they observed the driver, identified as “Jimmy Azcona” exit the vehicle and enter a bodega. After several minutes, “Jimmy Azcona” exited the bodega and

⁵ Please refer to case no.: 21-SW-490-PAS

eventually left the area, returning to [REDACTED]. Inspectors and Detective Coronado maintained surveillance at [REDACTED] and observed the Honda CRV RI reg. [REDACTED] 464 leave the residence. In the area of Public Street and Prairie Avenue, a marked RI State Police cruiser conducted a traffic stop on the Honda CRV RI reg. [REDACTED] 464. The driver of the Honda CRV RI reg. [REDACTED] 464 was identified as Duralline AZCONA RODRIGUEZ and was positively identified as SUSPECT 3. The RI State Police Trooper collected AZCONA RODRIGUEZ's personal information to include his phone number, which was [REDACTED]-6795. AZCONA RODRIGUEZ was issued a written warning for unlawful installation of sunscreen material.

27. A review of call records for [REDACTED]-7041 revealed there was one phone call to AZCONA RODRIGUEZ' phone on September 7, 2021.

28. Continued surveillance on AZCONA RODRIGUEZ and the Honda CRV RI reg. [REDACTED] 464 revealed a pattern of coming and going from [REDACTED] as well as coming and going from a Las Gigantes meat Market, located at [REDACTED], Providence.

29. On November 15, 2021, I learned a Priority Mail Express Parcel, tracking number EI110363798US, had been shipped from Puerto Rico to 2 Janes Street, Providence, Rhode Island (herein referred to as the JANES STREET PARCEL 2). I learned 2 Janes Street, Providence is a two-family home and the actual address is 2/4 Janes Street, Providence.

30. On November 16, 2021, the JANES STREET PARCEL 2 arrived, and it was addressed to "Evy j otero Apt 1 2 Janes ST Providence RI 02905-3225" with a return address of "Jose otero calle Fenix A17 carolina 00979." The JANES STREET PARCEL 2 was heavily taped on all creases and weighed four pounds 12 ounces. Utilizing USPS databases and Clear, I confirmed "calle Fenix A17 carolina 00979" was a legitimate address; however, the name "Jose otero" was not associated with that address. In regard to the recipient address, "Apt 1 2 Janes ST Providence RI 02905-3225", I confirmed it was a legitimate address and the name "Evy j otero" did in fact receive mail there.

31. On November 17, 2021, members of the USPIS Contraband Interdictions and Investigations (CI2) Task Force conducted a controlled delivery of JANES STREET PARCEL 2. At

approximately 10:08 am, Postal Inspector Michael Maccarone, acting in an undercover capacity as a USPS letter carrier, operating a USPS vehicle, delivered JANES STREET PARCEL 2. As Inspector Maccarone approached 2 Janes Street, Providence (herein referred to as the TARGET LOCATION), he noticed the front door to the TARGET LOCATION, was the left side door upon facing the residence. Inspector Maccarone scanned JANES STREET PARCEL 2 as delivered and placed it on the porch in front of the TARGET LOCATION's front door. As Inspector Maccarone was leaving the area, he observed parked in the driveway, a gray Honda Accord, Special Edition model, with tinted windows bearing a Delaware temporary license plate of [REDACTED] 2416 (herein referred to as the SUBJECT VEHICLE). Inspector Maccarone advised the SUBJECT VEHICLE matched the description of the Honda Accord that was involved in the robbery on September 18, 2021 which had a different Delaware temporary license plate.

32. After Inspector Maccarone left the area, Rhode Island State Police (RISP) Detective and USPIS Task Force Officer (TFO) Justin Andreozzi, observed a younger, light skinned Hispanic male wearing grey sweatpants, camouflage colored jacket and a rooster hat exit from the front door at 2 Janes Street and take custody of JANES STREET PARCEL 2. The younger Hispanic male (who would be later identified as Juan Bautista ROSARIO SANDOVAL) walked with JANES STREET PARCEL 2 towards the driveway where a dark grey, heavily tinted, Honda Accord was parked. ROSARIO SANDOVAL returned into the front door of 2 Janes Street without JANES STREET PARCEL 2. It should be noted that Detective Andreozzi had familiarized himself with images recorded by surveillance cameras of the robbery. From Detective Andreozzi's surveillance location, he was able to identify ROSARIO SANDOVAL as being involved in the letter carrier assault and larceny on September 18, 2021.

33. Detective Andreozzi advised a short time later, ROSARIO SANDOVAL left the TARGET LOCATION, walked back over to the driveway then returned to the TARGET LOCATION with JANES STREET PARCEL 2. Approximately 30 minutes later, ROSARIO SANDOVAL left the TARGET LOCATION, without JANES STREET PARCEL 2 and drove away in the SUBJECT VEHICLE. With the assistance of the RISP, the SUBJECT VEHICLE was

stopped in the area of [REDACTED], Providence, where the sole occupant, ROSARIO SANDOVAL was taken into custody.

34. ROSARIO SANDOVAL was transported to the USPIS office where he was interviewed. ROSARIO SANDOVAL did not speak English, so with assistance of RISP Corporal Daniel Hernandez, a certified Spanish speaker, ROSARIO SANDOVAL was read his constitutional rights, per the Miranda Decision. ROSARIO SANDOVAL advised he understood his rights and was willing to answer questions presented to him. ROSARIO SANDOVAL admitted he was involved with the assault and robbery of the letter carrier. ROSARIO SANDOVAL stated he would get paid a \$1000 from Jose Polanco, who was the individual who shipped the parcels. ROSARIO SANDOVAL stated the other individual, SUSPECT 2, who he referred to as "Wifey" was Jose Polanco's son and had come up on a bus from New York. ROSARIO SANDOVAL stated JANES STREET PARCEL 2 was the second parcel shipped to his address, along with the PMEP that was stolen on September 18, 2021. ROSARIO SANDOVAL stated AZCONA RODRIGUEZ worked at the bodega and was supposed to get paid \$300 to retrieve the PMEP on September 18th.

35. While ROSARIO SANDOVAL was being interviewed, RISP Detectives maintained surveillance at the TARGET LOCATION, when an individual identified as Nahun Martinez Guerrero (herein referred to as "MARTINEZ GUERRERO") arrived, driving a 2010 Honda Pilot and went into the TARGET LOCATION. Approximately four minutes later, MARTINEZ GUERRERO walked out of the TARGET LOCATION carrying a white trash bag and placed it in the front passenger seat of the Honda Pilot and began to leave. RISP Detectives stopped the vehicle and detained MARTINEZ GUERRERO. RISP Detectives could see inside the trash bag a USPS parcel with USPS tape on it.

36. MARTINEZ GUERRERO was transported to the USPIS office and interviewed. Again, with the assistance from RISP Corporal Daniel Hernandez, a certified Spanish speaker, MARTINEZ GUERRERO was read his constitutional rights per the Miranda Decision. MARTINEZ GUERRERO advised he understood his rights and was willing to answer questions presented to him. MARTINEZ GUERRERO stated he knows ROSARIO SANDOVAL but claimed

he did not live at his residence (the TARGET LOCATION). MARTINEZ GUERRERO stated he left for work this morning and was in N. Kingstown until 12 o'clock. MARTINEZ GUERRERO stated when he returned home he saw a trash bag sitting in the middle of his kitchen and knew it didn't belong to him. MARTINEZ GUERRERO stated he did not know why ROSARIO SANDOVAL was in his home but claimed he had come over yesterday to help fix something around the house. It should be noted, JANES STREET PARCEL 2 was scheduled to be delivered yesterday.

37. A review of the tracking details on the Honda CRV, RI reg. [REDACTED] 464 revealed the vehicle was in N. Kingstown this morning for several hours, parked on Compass Circle, where numerous warehouses were located.

IV. TRAINING AND EXPERIENCE ON DRUG OFFENSES

38. I have participated in the execution of numerous search warrants at the residences of drug-traffickers similar to the targets of this investigation. Based on my training and experience and familiarity with investigations into drug trafficking conducted by other law enforcement agents, I know the following:

a. Drug trafficking is a business that involves numerous co-conspirators, from lower-level dealers to higher-level suppliers, as well as associates to process, package, and deliver the drugs and launder the drug proceeds. Drug traffickers often travel by car, bus, train, or airplane, both domestically and to foreign countries, in connection with their illegal activities in order to meet with co-conspirators, conduct drug transactions, and transport drugs or drug proceeds.

b. Drug traffickers often maintain books, receipts, notes, ledgers, bank records, and other records relating to the manufacture, transportation, ordering, sale and distribution of illegal drugs. The aforementioned records are often maintained where drug traffickers have ready access to them, such as on their cell phones and other digital devices, and in their residences.

c. Communications between people buying and selling drugs take place by telephone calls and messages, such as e-mail, text messages, and social media messaging applications, sent to and from cell phones and other digital devices. This includes sending photos or videos of or related to the drugs between the seller and the buyer, the negotiation of price, and discussion of whether or not participants will bring weapons to a deal. In addition, it is common for

people engaged in drug trafficking to have photos and videos on their cell phones of drugs they or others working with them possess, as they frequently send these photos to each other and others to boast about the drugs or facilitate drug sales.

d. Drug traffickers often keep the names, addresses, and telephone numbers of their drug trafficking associates on their digital devices and in their residence. Drug traffickers often keep records of meetings with associates, customers, and suppliers on their digital devices and in their residence, including in the form of calendar entries and location data.

e. Drug traffickers often use vehicles to transport their narcotics and may keep stashs of narcotics in their vehicles in the event of an unexpected opportunity to sell narcotics arises.

f. Drug traffickers often maintain on hand large amounts of United States currency in order to maintain and finance their ongoing drug trafficking businesses, which operate on a cash basis. Such currency is often stored in their residences and vehicles.

g. Drug traffickers often keep drugs in places where they have ready access and control, such as at their residence or in safes. They also often keep other items related to their drug trafficking activities at their residence, such as digital scales, packaging materials, and proceeds of drug trafficking. These items are often small enough to be easily hidden and thus may be kept at a drug trafficker's residence even if the drug trafficker lives with others who may be unaware of his criminal activity.

h. It is common for drug traffickers to own multiple phones of varying sophistication and cost as a method to diversify communications between various customers and suppliers. These phones range from sophisticated smart phones using digital communications applications such as text messaging platforms (including SMS and MMS), iMessage, WhatsApp, Skype Messenger, Kik, Viber, Google Hangouts, and the like, to cheap, simple, and often prepaid flip phones, known colloquially as "drop phones," for actual voice communications.

i. It is common for drug traffickers to maintain personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the **TARGET LOCATION** and the **SUBJECT VEHICLE**. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

V. TRAINING AND EXPERIENCE ON DIGITAL DEVICES⁶

39. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law

⁶ As used herein, the term "digital device" includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

40. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during execution of a search warrant for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

41. The search warrant also requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.

b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.

c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the thumb- and/or fingers of the suspected user of that device(s) on the device(s); and (2) hold the device(s) in front of the face of the suspected user of that device(s) with the user's eyes open to activate the facial-, iris-, and/or retina-recognition feature.

VI. CONCLUSION

42. Further, based on these facts described above, I believe that the investigation has revealed that there is an ongoing, long-term, drug trafficking conspiracy in place and that ROSARIO SANDOVAL, AZCONA RODRIGUEZ, Nahun Martinez GUERRERO and other yet identified members of this conspiracy continue to engage violations of the SPECIFIED FEDERAL OFFENSES and that evidence of those offenses will be found in the TARGET LOCATION and SUBJECT VEHICLE. I therefore respectfully request that this Court issue search warrants authorizing the search of the locations described in Attachment A-1 thru A-2 and items described in Attachment B.

I declare that the foregoing is true and correct.


RICHARD F. ATWOOD
U.S. Postal Inspector

Richard Atwood
Postal Inspector
U.S. Postal Inspection Service

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

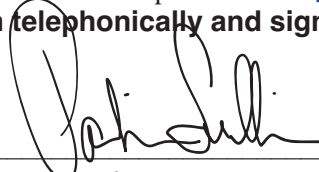
Sworn telephonically and signed electronically

November 17, 2021

Date

Providence, RI

City and State



Judge's signature

Patricia A. Sullivan, US Magistrate Judge

Printed name and title

ATTACHMENT A-1

PREMISES TO BE SEARCHED

The TARGET LOCATION is multi-family residence, which is addressed as 2/4 Janes Street, Providence, RI. The TARGET LOCATION is a multi-story building, beige in color with white trim. The front door to the TARGET LOCATION, is located on the left side when facing the residence and is white in color. The number “2” is located to the left of the TARGET LOCATION’s front door and is black in color. The mailbox, which is black and gold, is located to the left of the front door as well, affixed to the siding of the TARGET LOCATION.





ATTACHMENT A-2
PREMISES TO BE SEARCHED

The SUBJECT VEHICLE is a GRAY 2017 HONDA ACCORD, SPECIAL EDITION, VIN: 1HGCR2F16HA076280, Delaware temporary registration: [REDACTED] 4216.





ATTACHMENT B

I. ITEMS TO BE SEIZED

1. The items to be seized are evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, § 111(a) (Assaulting, resisting, or impeding certain officers or employees), Title 18, United States Code, § 2114(a) (assault with intent to rob mail matter) and Title 21, United States Code, Sections 841(a) (1) and 846 (drug trafficking and conspiracy).

(herein referred to as the SPECIFIED FEDERAL OFFENSES), namely:

- a) Weapons, to include firearms.
- b) Any controlled substance, controlled substance analogue, or listed chemical;
- c) Items and paraphernalia for the manufacturing, distributing, packaging, sale, or weighing of controlled substances, including scales and other weighing devices, plastic baggies, food saver sealing devices, heat sealing devices, balloons, packaging materials, containers, and money counters;
- d) Items used in the packaging of currency for consolidation and transportation, such as money-counting machines, money wrappers, carbon paper, rubber bands, duct tape or wrapping tape, plastic wrap or shrink wrap, and plastic sealing machines;
- e) United States currency over \$1,000 or bearer instruments worth over \$1,000 (including cashier's checks, traveler's checks, certificates of deposit, stock certificates, and bonds) (including the first \$1,000), and data, records, documents, or information (including electronic mail, messages over applications and social media, and photographs) pertaining to, obtaining, possessing, using, applications for, or transferring money over \$1,000, such as bank account records, cryptocurrency records and accounts;

FINANCIAL RECORDS: All financial records of or relating to ROSARIO SANDOVAL and others, and their nominees, assignees, or co-conspirators, including but not limited to financial

statements, balance sheets, income statements, cash flow statements, ledgers, journals, accounts receivable, accounts payable,

f) leases, bank statements, deposit tickets, deposit items, checks, checkbooks, check registers, passbooks, money orders, cashier's checks, official checks, bank drafts, wire transfer instructions and receipts, withdrawal slips, credit memos, debit memos, signature cards, account applications, automatic teller machine receipts, safe deposit box applications, safe deposit box keys, credit card statements, charge slips, receipts brokerage statements, buy and sell orders and other items evidencing the obtaining, secreting, transfer, or concealment of assets and the obtaining, secreting, transfer, concealment, or expenditure of money.

g) Items showing unexplained wealth or evidencing the proceeds derived from illicit drug trafficking, including but not limited to large sums of money, expensive vehicles, financial instruments, precious metals, jewelry, and real estate, and documents evidencing the procuring or leasing of these items.

h) Documents and records reflecting the identity of, contact information for, communications with, or times, dates or locations of meetings with co-conspirators, sources of supply of controlled substances, or drug customers, including calendars, address books, telephone or other contact lists, pay/owe records, distribution or customer lists, correspondence, receipts, records, and documents noting price, quantities, and/or times when drugs were bought, sold, or otherwise distributed, whether contained in hard copy correspondence, notes, emails, text messages, photographs, videos (including items stored on digital devices), or otherwise;

TRAVEL DOCUMENTS: All documents evidencing or relating to foreign or domestic travel of ROSARIO SANDOVAL, or their co-conspirators, including but not limited to airline tickets, tickets for other means of transport, credit card receipts, travel vouchers, hotel receipts, restaurant receipts, gas receipts, notes, schedules, other receipts evidencing travel, boarding passes, itineraries, luggage tags and receipts, frequent flyer statements and awards, car rental receipts and statements, photographs of travel locations, maps, written directions to a location, visas, passports, United States and foreign customs declaration receipts and forms.

i) Records, documents, programs, applications and materials, or evidence of the absence of same, sufficient to show call log information, including all telephone numbers dialed from any of the digital devices and all telephone numbers accessed through any push-to-talk functions, as well as all received or missed incoming calls;

j) STORAGE UNIT RECORDS: All records reflecting the ownership or control of storage units including keys, contracts, leases, payments, and inventories.

k) Shipping records, to include any and all receipts (USPS, FedEx, UPS, and DHL) for parcels shipped to and or from Puerto Rico.

l) Records, documents, programs, applications or materials, or evidence of the absence of same, sufficient to show SMS text, email communications or other text or written communications sent to or received from any of the digital devices and which relate to the above-named violation[s];

m) Records, documents, programs, applications or materials, or evidence of the absence of same, including text, instant, and social media messages (such as Facebook, Facebook Messenger, Snapchat, FaceTime, Skype, and WhatsApp), SMS text, email communications, or other text or written communications sent to or received from any digital device and which relate to the above-named violation[s];

n) Audio recordings, pictures, video recordings, or still captured images related to the purchase, sale, transportation, or distribution of drugs;

o) Contents of any calendar or date book;

p) Global Positioning System (“GPS”) coordinates and other information or records identifying travel routes, destinations, origination points, and other locations; and

q) Any digital device which is itself or which contains evidence, contraband, fruits, or instrumentalities of the SPECIFIED FEDERAL OFFENSES, and forensic copies thereof.

r) With respect to any digital device containing evidence falling within the scope of the foregoing categories of items to be seized:

i. evidence of who used, owned, or controlled the device at the time

the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs, and correspondence;

ii. evidence of the presence or absence of software that would allow others to control the device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. evidence of the attachment of other devices;

iv. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the device;

v. evidence of the times the device was used;

vi. passwords, encryption keys, biometric keys, and other access devices that may be necessary to access the device;

vii. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

viii. records of or information about Internet Protocol addresses used by the device;

ix. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used herein, the terms "records," "documents," "programs," "applications," and "materials" include records, documents, programs, applications, and materials created, modified,

or stored in any form, including in digital form on any digital device and any forensic copies thereof.

As used herein, the term “digital device” includes any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as telephone paging devices, beepers, mobile telephones, and smart phones; digital cameras; gaming consoles (including Sony PlayStations and Microsoft Xboxes); peripheral input/output devices, such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices, such as modems, routers, cables, and connections; storage media, such as hard disk drives, memory cards, and security devices.

II. SEARCH PROCEDURE FOR DIGITAL DEVICE(S)

In searching digital devices (or forensic copies thereof), law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel (the “search team”) will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) and/or forensic image(s) thereof to an appropriate law enforcement laboratory or similar facility to be searched at that location.

b. The search team will conduct the search only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The search team may subject all of the data contained in each digital device capable of containing any of the items to be seized to the search protocols to determine whether the device and any data thereon falls within the list of items to be seized. The search team may also search for and attempt to recover deleted, “hidden,” or encrypted data to determine, pursuant to the search protocols, whether the data falls within the list of items to be seized.

ii. The search team may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

iii. The search team may use forensic examination and searching tools, such as “EnCase” and “FTK” (Forensic Tool Kit), which tools may use hashing and other sophisticated techniques.

c. If the search team, while searching a digital device, encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that device pending further order of the Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

d. If the search determines that a digital device does not contain any data falling within the list of items to be seized, the government will, as soon as is practicable, return the device and delete or destroy all forensic copies thereof.

e. If the search determines that a digital device does contain data falling within the list of items to be seized, the government may make and retain copies of such data, and may access such data at any time.

f. If the search determines that a digital device is (1) itself an item to be seized and/or (2) contains data falling within the list of other items to be seized, the government may retain the digital device and any forensic copies of the digital device, but may not access data falling outside the scope of the other items to be seized (after the time for searching the device has expired) absent further court order.

g. The government may also retain a digital device if the government, prior to the end of the search period, obtains an order from the Court authorizing retention of the device (or while an application for such an order is pending), including in circumstances where

the government has not been able to fully search a device because the device or files contained therein is/are encrypted.

h. After the completion of the search of the digital devices, the government shall not access digital data falling outside the scope of the items to be seized absent further order of the Court.

In order to search for data capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items:

- a. Any digital device capable of being used to commit, further, or store evidence of the offense(s) listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding, or storage of digital data;
- c. Any magnetic, electronic, or other storage device capable of storing digital data;
- d. Any documentation, operating logs, or reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters, or other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles, or similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, [biometric keys,] test keys, encryption codes, or other information necessary to access the digital device or data stored on the digital device.
- h. During the execution of this search warrant, law enforcement is permitted to: (1) depress the USER's thumb- and/or fingers onto the fingerprint sensor of the device (only when the device has such a sensor), and direct which specific finger(s) and/or thumb(s) shall be depressed; and (2) hold the device in front of the USER's face with his or her eyes

open to activate the facial-, iris-, or retina-recognition feature, in order to gain access to the contents of any such device.